Fortify Scan Issue: Old version of rulepacks used during scan

⚠️ **This page has been made public for vendors**

Question

What does the Fortify scan issue "Old version of rulepacks used during scan" mean, how can I detect it, and how can I fix it?

Answer

This scan issue indicates that an old version of the Fortify rulepacks was used to perform the code scan. The rulepacks encode the security knowledge that Fortify applies to the code, therefore scans must be performed with the most recent version of the rulepacks to ensure the most complete security knowledge is applied to the scan. Scans that do not use the most recent rulepacks may not include a complete set of results

How to detect

The most reliable way to determine whether or not your rulepacks are up-to-date is to try to update them before performing a scan. Details on how to accomplish that are described in the "how to resolve" section below.

There are two steps to manually determine if you have the most recent version of the Fortify rulepacks:

1. Determine the current version of the rulepacks. Rulepack updates are announced on the OISSWA Blog and the VA Software Assurance Newsletter (signup for the newsletter HERE)
2. Check the version number of the rulepacks you are using.

   - If looking at a scan of the code, go to the Project Summary page, select the Analysis Information tab and the Security Content sub-tab. This will show the versions of the rulepacks used for the scan.
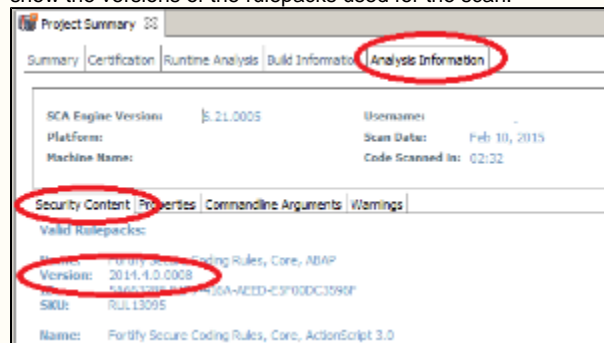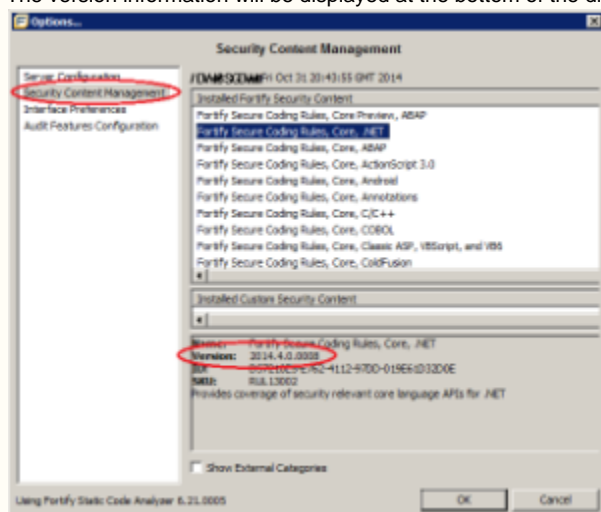

   - Alternatively, open the Optiions dialog (Options->Options in Audit Workbench, HP Fortify->Options in Visual Studio and Eclipse), select

HPE Fortify Version	4.30 and later
Programming Language	☑ C/C++ ☑ .NET ☑ Java ☑ Objective-C ☑ Other
Fortify Audit Workbench	☑ Yes ☐ No
Fortify IDE Plugin	☑ Yes ☐ No
Other Fortify Component	☑ Yes ☐ No

*Request code review tools, validations, and support HERE.*

the Security Content Management tab and select one of the rulepacks. The version information will be displayed at the bottom of the dialog.

How to resolve

To fix this issue, update the Fortify rulepacks and rerun the scan. Note that after you rerun the scan, you can merge your previous results into the new scan to carry any previous audits to the new scan.

The rulepacks may be updated either using the fortifyupdate command-line tool (found in the <fortify install dir>/bin directory) or they may be updated from the graphical user interface. To update from the GUI, open the Optiions dialog (Options->Options in Audit Workbench, HP Fortify->Options in Visual Studio and Eclipse), select the Security Content Management tab and click on the "Update Security Content" button.
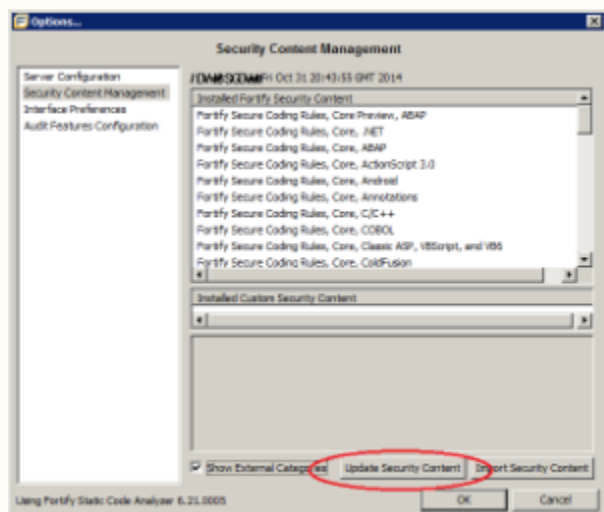
The technical note How to install or update Fortify rulepacks provides more information on how to update the rulepacks.

References

- **VA Top 10 Fortify Scan Issues For 2016 (Q4)**
- **VA Top 10 Fortify Scan Issues For 2016 (Q3)**
- **VA Top 10 Fortify Scan Issues For 2016 (Q2)**
- **VA Top 10 Fortify Scan Issues For 2016 (Q1)**
- **VA Top 10 Fortify Scan Issues For 2015 (Q4)**
- **VA Top 10 Fortify Scan Issues For 2014 (Q3)**
- **VA Top 10 Fortify Scan Issues For 2015 (Q2)**
- **VA Top 10 Fortify Scan Issues For 2015 (Q1)**